AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS

1. (Original) A method of backing up one or more files on a local device onto remote servers over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.

2. (Original) The invention of claim 1 wherein the bundle is encrypted using a strong block cipher.

3. (Original) The invention of claim 1 wherein the authentication code is an HMAC.

4. (Original) The invention of claim 1 wherein the cryptographic keys contain at least 128 bits.

5. (Currently Amended) A method of restoring one or more files on remote servers to a local device over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key;

and

decompressing one or more files from the bundle[[;]].

6. (Original) The invention of claim 5 wherein the bundle was encrypted using a strong block cipher.

7. (Original) The invention of claim 5 wherein the authentication code is an HMAC.

8. (Original) The invention of claim 5 wherein the cryptographic keys contain at least 128 bits.

9. (Original) A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.

10. (Original) The invention of claim 9 wherein the bundle is encrypted using a strong block cipher.

11. (Original) The invention of claim 9 wherein the authentication code is an HMAC.

12. (Original) The invention of claim 9 wherein the cryptographic keys contain at least 128 bits.

13. (Currently amended) A device-readable medium storing program instructions for

performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key; and

decompressing one or more files from the bundle[[;]].

14. (Original) The invention of claim 13 wherein the bundle was encrypted using a strong block cipher.

15. (Original) The invention of claim 13 wherein the authentication code is an HMAC.

16. (Original) The invention of claim 13 wherein the cryptographic keys contain at least 128 bits.